EXHIBIT 3

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

SETTLEMENT AGREEMENT

This settlement agreement (the "Agreement") with respect to **COMPL-[redacted]** is made by and between the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and Binance Holdings, Ltd. ("Binance") and any of its assignees, parent corporations, subsidiaries, affiliates involved in the operation of the Binance.com exchange, successors-in-interest, and transferees (collectively referred to hereafter as "Respondent").

I. PARTIES

OFAC administers and enforces economic sanctions against targeted foreign countries, regimes, terrorists, international narcotics traffickers, and proliferators of weapons of mass destruction, among others. OFAC acts under Presidential national emergency authorities, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction.

Respondent's affiliates operate the largest virtual currency exchange in the world by volume. Binance's primary online virtual currency exchange is operated on the Binance.com platform, where users may trade fiat or virtual currency (*e.g.*, bitcoin) through a variety of arrangements, including spot, futures, derivatives, and margin trading. At the time of the conduct at issue, the Binance platform used an algorithmic matching engine to facilitate trades based on price and time, without controls to prevent U.S. users from trading with blocked persons or persons in sanctioned jurisdictions.

II. APPARENT VIOLATIONS

From approximately August 2017 to October 2022 (the "Relevant Period"), Respondent matched and executed virtual currency trades on its online exchange platform between U.S. person users and users in sanctioned jurisdictions or blocked persons. In doing so, Respondent appears to have violated multiple OFAC sanctions prohibitions across various U.S. sanctions programs when, among other things, it (i) engaged in the direct or indirect exportation or other supply of goods and services from the United States, or by U.S. persons, to users whom Respondent identified through its Know Your Customer (KYC) process, Internet Protocol (IP) address, phone number or other means, as being located in Iran, Syria, North Korea, the Crimea Region of Ukraine, Cuba, the so-called Donetsk People's Republic ("DNR"), the so-called Luhansk People's Republic ("LNR"), or blocked; and (ii) caused U.S. persons to engage directly or indirectly in transactions with users located in Iran, Syria, North Korea, the Crimea Region of Ukraine, Cuba, the DNR, the LNR, or blocked persons, by matching such U.S. users to parties in sanctioned jurisdictions or blocked persons.

This conduct resulted in at least 1,667,153 virtual currency transactions — totaling approximately $706,068,127 — in apparent violation of the below U.S. sanctions programs (the "Apparent Violations"). The maximum statutory penalty amount for these violations is

$592,133,829,398. Specifically, during the Relevant Period the Respondent engaged in the following Apparent Violations:

1. *Iran*: Respondent matched and executed 1,205,784 trades totaling $599,515,938 in virtual currency and futures products between U.S. persons and persons located in Iran in apparent violation of the prohibition against the direct or indirect exportation, reexportation, sale or supply of goods or services to Iran, § 560.204 of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560 (ITSR), and the prohibition against causing violations of the ITSR, 31 C.F.R. § 560.203;

2. *Syria*: Respondent matched and executed 42,609 trades totaling $17,965,226 in virtual currency and futures products between U.S. persons and persons located in Syria in apparent violation of the prohibition against the direct or indirect exportation, reexportation, sale or supply of goods or services to Syria, § 542.207 of the Syrian Sanctions Regulations, 31 C.F.R. part 542;

3. *North Korea*: Respondent matched and executed 80 trades totaling $43,745.88 in virtual currency between U.S. persons and persons located in North Korea in apparent violation of the prohibitions against the direct or indirect exportation or reexportation of goods or services to North Korea, § 3(a) of Executive Order ("E.O.") 13722 of March 15, 2016 ("E.O. 13722"), and § 510.206 of the North Korea Sanctions Regulations, 31 C.F.R. part 510 (NKSR), and the prohibitions against causing a violation of E.O. 13722 or the NKSR, § 7(a) of E.O. 13722 and 31 C.F.R. § 510.212;

4. *Crimea Region of Ukraine*: Respondent matched and executed 409,295 trades totaling $86,977,789 in virtual currency and futures products between U.S. persons and persons located in the Crimea Region of Ukraine in apparent violation of the prohibitions against the direct or indirect exportation, reexportation, sale or supply of goods or services to the Crimea Region of Ukraine, § 1(a)(iii) of E.O. 13685 of December 19, 2014 ("E.O. 13685"), and § 589.207 of the Ukraine-/Russia-Related Sanctions Regulations, 31. C.F.R. part 589 (URSR), and the prohibitions against causing a violation of E.O. 13685 or the URSR, § 3(a) of E.O. 13685 and 31 C.F.R. § 589.213;

5. *Cuba:* Respondent matched and executed 9,315 trades, totaling $1,535,225, in virtual currency and futures products between U.S. persons and persons located in Cuba, in apparent violation of the prohibition on the transfer of property or property interests subject to U.S. jurisdiction in which Cuban nationals have an interest, § 515.201 of the Cuban Assets Control Regulations, 31 C.F.R. part 515;

6. *LNR and DNR:* Respondent matched and executed 68 trades, totaling $14,159, in virtual currency and futures products between U.S. persons and persons located in the LNR and DNR, in apparent violation of the prohibition against the direct or indirect exportation, reexportation, sale or supply of goods or services to the LNR or DNR, § 1(a)(iii) of E.O. 14065 of February 21, 2022 ("E.O. 14065"), and the prohibition against causing a violation of E.O. 14065, § 4(a) of E.O. 14065; and

7. *Blocked Persons:* Respondent matched and executed two trades, totaling $16,043, in futures products between U.S. persons and persons whose property and interests in property are blocked pursuant to § 594.201(a) of the Global Terrorism Sanctions Regulations, 31 C.F.R. part 594, causing U.S. persons to engage in transactions or dealings in the property or interests in property of such blocked persons, in apparent violation of Section 206(a) of the International Emergency Economic Powers Act, 50 U.S.C. § 1701 et seq.

III. FACTUAL STATEMENT

Binance was founded in 2017, and by March 2018 was running the largest virtual currency exchange in the world by trading volume. Binance's primary online virtual currency exchange is operated on the Binance.com platform where users may trade fiat or virtual currency (*e.g.*, bitcoin) through a variety of arrangements, including spot, futures, derivatives, and margin trading. To use Binance, a user must first open a Binance account and then fund the account by depositing assets, either through a virtual currency or fiat currency deposit. Upon onboarding, Binance users can transact in hundreds of virtual currencies and financial products using the funds in their Binance-hosted "wallets." Binance user funds are held in omnibus digital wallets that are visible on the blockchain. Users' funds are accounted for via an internal Binance ledger, and Binance acts as the custodian of user funds.

In general, Binance users trade by submitting orders to Binance to buy or sell virtual currency or virtual currency products. Binance's algorithmic matching engines ingest incoming buy/sell orders and match them with pending orders on Binance's orderbook solely according to price and time. Binance then records each transaction in its internal ledger and credits or debits users' Binance accounts to reflect the transaction. Transactions between Binance users do not occur on, and are not recorded on, the blockchain. As described below, Binance knew or had reason to know the location of its user base, including the fact that it was matching users located in the United States with counterparties in sanctioned jurisdictions or blocked persons.

In 2018, Binance began to develop its first sanctions-related compliance plans and procedures, including hiring a Chief Compliance Officer (CCO) in April 2018. The next month, in May 2018, Binance issued a public statement on sanctions compliance when it updated its Terms of Use to explain that by using the platform users acknowledged and declared themselves not to be on "any economic sanctions list." The Terms of Use also stated that Binance "may restrict or deny its services to sanctioned countries." In June and July 2018, Binance issued compliance policies, including a Global Compliance Policy, which stated that Binance "adheres to the Sanctions list maintained by the Office of Foreign Assets Control" and that "Binance will not conduct business with any personnel, entities or countries listed in the Sanctions list under any conditions." In October 2018, Binance updated its policy, which by its terms prohibited new users from sanctioned and other high-risk jurisdictions, including Iran, Syria, North Korea, and Cuba.

Following issuance of these policies, Binance began taking steps to identify sanctioned jurisdiction users for offboarding. Efforts to offboard these users, however, were implemented

inadequately, at least in part due to Binance senior management decisions to appear compliant while disregarding known sanctions risks.

Communications from senior management demonstrate their awareness that servicing users from sanctioned jurisdictions could cause a violation of U.S. sanctions regulations. For example, in an October 18, 2018, message regarding the potential blocking of sanctioned country IP addresses, the then CCO informed Binance's Chief Executive Officer (CEO) that "we currently have users from sanction[ed] countries on [Binance.com]," adding that the "[d]ownside risk is if fincen or ofac has concrete evidence we have sanction[ed] users, they might try to investigate or blow it up big on worldstage." In another communication, the then CCO stated that the CEO "made a decision to IP block sanction countries." In response, an employee explained in an internal chat conversation that "Blocking IPs [is] just [the] cost of building long-term sustainable business in US. Also needed to sell to large traders/institutional clients in US."

Further indicating understanding of the sanctions risk presented by Binance's operations, the then CCO in October 2018 explained to Binance employees that "they all just remove mention of [sanctioned country] names and no support but NEVER REMOVE sanction users already on our .com." The then CCO made clear that compliance was to first scrub Binance.com of all reference to and support for sanctioned jurisdictions before turning to address the underlying sanctions risk by blocking IP addresses associated with sanctioned jurisdictions.

In June 2019, the CEO demonstrated his own broad awareness of U.S. sanctions prohibitions applicable to Binance when he told a senior Binance employee that "the U.S. has this law: you have to prevent Americans and any terrorists from doing any transactions. In order [for America] to accomplish this, if you serve Americans or service American sanctioned countries, you have to give your data to the American regulators." He added, "the U.S. says we are not focusing on the dollar; if our citizens use your services we can arrest/catch you."

In June 2019, Respondent announced the launch of a new U.S.-based exchange, called Binance.US. After Binance.US was launched in September 2019, the then CCO wrote to a senior employee on October 31, 2019 that "[t]he ofac regulation clearly states U.S. Persons, doing biz with OFAC is wrong," adding, "so back to the clean block of U.S. persons on [Binance].com that effectively mitigates the OFAC risk to a minimal." The then CCO also stated that it was a priority to convince the CEO to "to do a clean block on US for [Binance].com." That is, one benefit of the creation of Binance.US was that it would minimize sanctions compliance risk by moving U.S. users off the Binance.com platform.

Binance, however, continued to rely heavily on its U.S. user base for a substantial portion of its trading volume and liquidity. Notwithstanding the launch of Binance.US in September 2019, Binance did not implement IP blocking of U.S. users until April 2021, in part to continue benefiting from the trading activity of U.S. users.

Even after Binance began to take steps to offboard U.S. users from the Binance.com platform, the company retained lucrative high volume and liquidity-providing U.S. users on Binance.com to boost the company's revenue. As late as July 2020, in response to a question from a Binance employee about how to onboard a new U.S. user, the then CCO stated, "we ask

them to onboard with [Binance.]US, and then if their volume is really very big, we will push hard on [the] .com side to accept it on an exceptional basis." Thus, Binance allowed U.S. users to continue transacting on the Binance.com platform with inadequate controls in place to prevent those users from trading with users in sanctioned countries and blocked persons.

One way that Binance sought to foster the appearance of effective compliance controls, while in fact retaining U.S. users and sanctioned jurisdiction users on its platform, was to suggest its users utilize Virtual Private Networks ("VPNs") that could circumvent Binance's geofencing controls, *i.e.*, technical protocols that blocked access for users with IP addresses from the United States and sanctioned jurisdictions. For example, in May 2019, as the management team discussed blocking U.S. IP addresses ahead of the Binance.US launch, the CEO stated that a very specific popup notice should appear for U.S. users trying to access a non-U.S. Binance platform, adding, "I'll have a look at it myself. We need to word it very carefully so that we let people know what they need to do, including using a VPN, without explicitly stating it."

On February 12, 2020, the then CCO stressed to another Binance employee that the presence of U.S. users on the Binance.com platform would expose Binance to legal risk under laws and regulations administered and enforced by OFAC and other U.S. regulatory agencies, stating, "if US users get on [Binance].com we become subjected to the following US regulators, fincen ofac and SEC." He added, however, that Binance.com tried to ask U.S. users to "use VPN," "provide . . .non-US documents," or "get them through other creative means."

As a result of the conduct described above, between approximately August 2017 and October 2022, Binance processed 1,667,153 virtual currency transactions — totaling approximately $706,068,127 — in apparent violation of numerous U.S. sanctions programs.

IV. TERMS OF SETTLEMENT

OFAC and Respondent agree as follows:

1. In consideration of the undertakings of Respondent in paragraph 2 below, and subject to the breach provisions of this Agreement, OFAC agrees to a settlement in the amount of $968,618,825 and to release and forever discharge Respondent, without any finding of fault, from any and all civil liability in connection with the Apparent Violations arising under the legal authorities that OFAC administers. Respondent's obligation to pay OFAC the portion of this settlement totaling $898,618,825 arising from certain apparent violations of the ITSR shall be deemed satisfied up to an equal amount by payments in satisfaction of Respondent's obligations under its plea agreement with the U.S. Department of Justice (the "plea agreement") dated on or around November 21, 2023 arising out of the same conduct, such that Respondent is obligated to pay $70,000,000 to the U.S. Department of the Treasury pursuant to this settlement.

2. In consideration of the undertakings of OFAC in paragraph 1 above, Respondent agrees and represents:

A. Pursuant to the dates specified in paragraph 14.a of the plea agreement entered into by Binance with the Department of Justice, to:

   (i) sign, date, and email the Agreement to: [redacted] at [redacted] Office of Foreign Assets Control, Freedman's Bank Building, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220; and

   (ii) pay or arrange for the payment to the U.S. Department of the Treasury (the "Department") the amount of $70,000,000. Respondent's payment must be made either by electronic funds transfer in accordance with the enclosed "Electronic Funds Transfer (EFT) Instructions," or by cashier's or certified check or money order payable to the "U.S. Treasury" and referencing **COMPL[redacted]** Unless otherwise arranged with the Department's Bureau of the Fiscal Service, Respondent must either: (1) indicate payment by electronic funds transfer, by checking the box on the signature page of this Agreement; or (2) enclose with this Agreement the payment by cashier's or certified check or money order.

B. To waive (i) any claim or defense by or on behalf of Respondent, whether asserted or unasserted, against OFAC, the Department, or its officials and employees arising out of the facts giving rise to the enforcement matter that resulted in this Agreement, including but not limited to OFAC's investigation of the Apparent Violations, and (ii) any possible legal objection to this Agreement at any future date.

C. **Compliance Commitments:** By entering into this Agreement, Respondent and Respondent's senior management, including the Chief Executive Officer, recognizes the seriousness of apparent violations of the laws and regulations administered by OFAC and acknowledges Respondent and senior management's understanding of the apparent violations at issue. Respondent has terminated the apparently violative conduct described above; has implemented a sanctions compliance program; and will maintain sanctions compliance measures that are designed to minimize the risk of recurrence of similar conduct in the future for at least five years following the execution date of this Agreement. Specifically, as part of these sanctions compliance measures, Respondent agrees to the following Compliance Commitments:

   a. **Management Commitment:**

      i. Senior management, including the Chief Executive Officer, has reviewed and approved Respondent's sanctions compliance program, including enhancements implemented in response to the Apparent Violations and related sanctions compliance risk.

      ii. Respondent's compliance unit(s) is (are) delegated sufficient authority and autonomy to deploy its policies and procedures in a manner that effectively controls Respondent's sanctions risk.

iii. Respondent's compliance unit(s) receives (receive) adequate resources — including in the form of human capital, expertise, information technology, and other resources, as appropriate — that are relative to Respondent's breadth of operations, target and secondary markets, and other factors affecting its overall risk profile.

iv. Respondent's senior management, including the Chief Executive Officer promotes a "culture of compliance" throughout the organization.

v. Respondent's senior management will implement necessary measures to reduce the risk of recurrence of apparent violations in the future.

b. **Risk Assessment:**

i. Respondent conducts an OFAC risk assessment in a manner, and with a frequency, that adequately accounts for potential sanctions compliance risks. Such risks could be posed by its clients and customers, products, services, supply chain, intermediaries, counterparties, transactions, or geographic locations, depending on the nature of the organization.

ii. Respondent has developed a methodology to identify, analyze, and address the particular risks. The risk assessments will be updated to account for the conduct and root causes of any apparent violations or systemic deficiencies identified by Respondent during the routine course of business, for example, through a testing or audit function.

iii. Specifically, Respondent has implemented new compliance policies and procedures that require annual enterprise-wide risk assessment to identify and mitigate compliance risks, including sanctions risk.

c. **Internal Controls:**

i. Respondent has designed and implemented written policies and procedures outlining its sanctions compliance program. These policies and procedures are relevant to the organization, capture Respondent's day-to-day operations and procedures, are easy to follow, and designed to prevent employees from engaging in misconduct.

ii. Respondent has implemented internal controls that adequately address the results of its sanctions risk assessment and profile. These internal controls should enable Respondent to clearly and effectively identify, interdict, escalate, and report to appropriate personnel within the organization transactions and activity that may be prohibited by OFAC. To the extent information technology solutions factor into Respondent's internal controls, Respondent has selected and calibrated the solutions in a manner that is

appropriate to address Respondent's risk profile and compliance needs, and Respondent routinely tests the solutions to ensure effectiveness.

iii. Respondent will enforce the policies and procedures it implements as part of its sanctions compliance internal controls through regular internal or external audits.

iv. Respondent's OFAC-related recordkeeping policies and procedures will adequately account for its requirements pursuant to the sanctions programs administered by OFAC.

v. Upon learning of a weakness in its internal controls pertaining to sanctions compliance, Respondent will take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.

vi. Respondent has clearly communicated the sanctions compliance program's policies and procedures to all relevant staff, including personnel within the sanctions compliance program, as well as relevant gatekeepers and business units operating in high-risk areas (e.g., customer acquisition, payments, sales, etc.) and to external parties performing sanctions compliance responsibilities on behalf of Respondent.

vii. Respondent has appointed personnel to integrate the sanctions compliance program's policies and procedures into Respondent's daily operations. This process includes consultations with relevant business units and confirms that Respondent's employees understand the policies and procedures.

viii. Specifically, Respondent has revised and updated compliance policies and procedures, to include the use of improved internal controls such as user and transaction-level screening, geolocation tools, and additional risk-based know-your-customer due diligence, and other reviews of new and existing users. In addition, Respondent has conducted lookback reviews of users to identify and offboard users from the United States as well as sanctioned jurisdictions.

d. **Testing and Audit:**

i. Respondent will ensure that the testing or audit function is accountable to senior management, is independent of the audited activities and functions, and has sufficient authority, skills, expertise, resources, and authority within the organization.

ii. Respondent will ensure that it employs testing or audit procedures appropriate to the level and sophistication of its sanctions compliance program and that this function, whether deployed internally or by an external party, reflects a

comprehensive and objective assessment of Respondent's sanctions-related risks and internal controls.

iii. Respondent will ensure that, upon learning of a confirmed negative testing result or audit finding pertaining to its sanctions compliance program, it will take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.

iv. Specifically, Respondent will contract with third-party firms to complete audits and reviews of Respondent's internal controls, policies, and procedures.

e. **Training:**

i. Respondent will ensure that its OFAC-related training program provides adequate information and instruction to employees and, as appropriate, stakeholders (for example, clients, suppliers, business partners, and counterparties) in order to support Respondent's sanctions compliance efforts.

ii. Respondent will provide OFAC-related training with a scope that is appropriate for the products and services that Respondent offers; the customers, clients, and partner relationships it maintains; and the geographic regions in which it operates.

iii. Respondent will provide OFAC-related training with a frequency that is appropriate based on its OFAC risk assessment and risk profile and, at a minimum, at least once a year to all relevant employees.

iv. Upon learning of a confirmed negative testing result or audit finding, or other deficiency pertaining to its sanctions compliance program, Respondent will take immediate and effective action to provide training to relevant personnel.

v. Respondent will ensure that its training program includes easily accessible resources and materials that are available to all applicable personnel.

vi. Specifically, Respondent has provided enhanced training for its employees both internally and by contracting with third-party firms.

f. **Cooperation with OFAC:** Respondent agrees to cooperate fully with OFAC in any and all matters under investigation by OFAC, including any investigation of Respondent, its subsidiaries or affiliates, or any of its present or former officers, directors, employees, agents, and consultants, or any other party. Respondent agrees that its cooperation pursuant to this paragraph shall include, but not be limited to, timely providing upon request, as determined by OFAC, any information, testimony, document, record, or other tangible evidence about which OFAC may inquire of Respondent, as well as making available for interviews or

testimony any present or former officers, directors, employees, agents, and consultants of the Respondent to the extent permitted by law. This obligation includes, but is not limited to, sworn testimony pursuant to an administrative subpoena or a request for information. Respondent further agrees that it shall timely and truthfully disclose, as determined by OFAC, all evidence and factual information related to any conduct or activities of Respondent, its subsidiaries and affiliates, and those of its present and former directors, officers, employees, agents, and consultants, that may constitute a violation of U.S. economic sanctions.

g. **Independent Compliance Monitor:** Respondent undertakes to engage an Independent Compliance Monitor (the "Monitor") for a five-year term pursuant to the provisions set forth in the consent order between Respondent and the Financial Crimes Enforcement Network (FinCEN), dated on or around November 21, 2023, and in the plea agreement, dated on or around November 21, 2023. Respondent agrees that its undertakings and obligations with respect to the Monitor under the FinCEN consent order and the plea agreement are incorporated by reference into this Agreement as a Compliance Commitment. Respondent further agrees that the Monitor's mandate under the FinCEN consent order and the plea agreement shall include review and assessment of Respondent's compliance with U.S. economic sanctions and the effectiveness of Respondent's sanctions compliance program, and its adherence to the above Compliance Commitments. Accordingly, Respondent agrees that each of the Monitor's work plans, reviews, and reports during the applicable term of the Monitor's engagement shall address, among other things, the Monitor's review and assessment of Respondent's sanctions compliance program, including Respondent's adherence to the Compliance Commitments described herein.

h. **Annual Certification:** On an annual basis, for a period of five years, starting from 180 days after the date this Agreement is executed, a senior-level executive of Respondent shall submit to OFAC a written explanation that provides substantive details regarding how Respondent is meeting all the Compliance Commitments detailed in this Subparagraph 2.C of this Agreement, including its undertaking with respect to the Monitor.

D. Should OFAC have reason to believe that a material breach of, or misrepresentation in or pursuant to, this Agreement has occurred, including due to a failure to specifically perform or fulfill completely each of Respondent's Compliance Commitments, OFAC shall provide written notice to Respondent of the breach or misrepresentations and provide Respondent with 45 days from the date of Respondent's receipt of such notice, or longer as determined by OFAC, to provide a response demonstrating that no material breach or misrepresentation has occurred or that any breach or misrepresentation has been cured.

E. If, after receiving such response, OFAC determines, in its sole discretion, that a material breach of, or misrepresentation in, or pursuant to, this Agreement has

occurred, including due to a failure to specifically perform or fulfill completely each of Respondent's Compliance Commitments, OFAC will provide notice to Respondent of its determination. In such event, OFAC may re-open its investigation with respect to the Apparent Violations and may seek to impose on Respondent a civil monetary penalty in an amount up to the applicable statutory maximum. Any such investigation may be premised on information provided by Respondent or its present or former officers, directors, employees, agents, and consultants, or any other party.

F. The statute of limitations applying to the Apparent Violations shall be deemed tolled until a date 360 days following Respondent's receipt of notice of OFAC's determination that a breach of, or misrepresentation in, this Agreement has occurred.

G. Should the Respondent engage in any violations of the sanctions laws and regulations administered by OFAC — including those that are either apparent or alleged — OFAC may consider Respondent's sanctions history, or its failure to employ an adequate sanctions compliance program or appropriate remedial measures, associated with this Agreement as a potential aggravating factor consistent with the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, Appendix A.

3. This Agreement does not constitute a final agency determination that a violation has occurred and shall not in any way be construed as an admission by Respondent that Respondent engaged in the Apparent Violations.

4. This Agreement has no bearing on any past, present, or future OFAC actions, including the imposition of civil monetary penalties, with respect to any activities by Respondent other than those set forth in the Apparent Violations.

5. OFAC may, in its sole discretion, post on OFAC's website this entire Agreement and/or issue a public statement about the factors of this Agreement, including the identity of any entities involved, the settlement amount, and a brief description of the Apparent Violations.

6. The certifications to OFAC required under this Agreement shall be submitted to OFAC by email at OFAC_Compliance_Certification@treasury.gov, addressed to Assistant Director, Enforcement Division, Office of Foreign Assets Control, Freedman's Bank Building, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

7. This Agreement consists of 12 pages and expresses the complete understanding of OFAC and Respondent regarding resolution of OFAC's enforcement matter involving the Apparent Violations. No other agreements, oral or written, exist between OFAC and Respondent regarding resolution of this matter.

8. Respondent agrees that if a court of competent jurisdiction considers any of the provisions of this Agreement unenforceable, such unenforceability does not render the entire Agreement unenforceable. Rather, the entire Agreement will be construed as if not

containing the particular unenforceable provision(s), and the rights and obligations of OFAC and Respondent shall be construed and enforced accordingly.

9. This Agreement shall inure to the benefit of and be binding on each party, as well as its respective successors or assigns. Respondent agrees that the provisions of this Agreement are binding on its owners, officers, employees, agents, representatives, affiliates, successors, assigns, and transferees to whom Respondent agrees to provide a copy of the executed Agreement. Should Respondent seek to sell, merge, transfer, or assign its operations, or any portion thereof, that are the subject of this Agreement, Respondent must, as a condition of sale, merger, transfer, or assignment obtain the written agreement of the buyer, merging entity, transferee, or assignee to comply with this Agreement.

10. Respondent's Duly Authorized Representative, by signing this Agreement, hereby represents and warrants that the Duly Authorized Representative has full power and authority to execute and agree to this Agreement for and on behalf of Respondent, and further represents and warrants that Respondent agrees to be bound by the terms and conditions of this Agreement.

Respondent accepts the terms of this Agreement on this 21st day of **November, 2023**

Signature

Joshua Eaton
Respondent's Printed Name (or in the case of an entity, the name of Respondent's Duly Authorized Representative)

Deputy General Counsel
Printed Title of Respondent's Duly Authorized Representative and Name of Entity (if applicable)

Please check this box if you have not enclosed payment with this Agreement and will instead be paying or have paid by electronic funds transfer (see paragraph 2(A)(ii) and the EFT Instructions enclosed with this Agreement).

Date: November 21, 2023

Bradley T. Smith
Digitally signed by Bradley T. Smith
Date: 2023.11.21 12:43:55 -05'00'

Bradley T. Smith
Director
Office of Foreign Assets Control